

Belangrijke tips:

Installeer updates. Dit is de belangrijkste bescherming tegen hackers. Hoe ouder je software, hoe makkelijker hackers toegang krijgen tot je apparaten.

Gebruik unieke wachtwoorden voor elke website of app. Om de wachtwoorden niet te vergeten kun je deze veilig opslaan in een wachtwoordmanager, bijvoorbeeld: LastPass of KeePass.

Activeer tweestapsverificatie. Bij tweestapsverificatie voeg je een extra beveiligingslaag toe aan je account. Toegangscode worden naar een vertrouwd apparaat gestuurd om in te kunnen loggen.

Maak back-ups. Het valt aan te raden om zowel een online als offline back-up te maken. Een online back-up maak je met een clouddienst als Dropbox of Stack, een offline back-up via een externe harde schijf.

Kijk uit met openbare oplaadpunten. Het gebruik van publiek toegankelijke USB-poorten is niet zonder risico. Maak gebruik van de USB data blocker om veilig je mobiele apparaten op te laden.

**Laat Je Niet
Hack Maken**



Meer tips? Ga naar LaatJeNietHackMaken.nl. Deze gratis digitale handleiding legt op een begrijpelijke manier uit hoe je jezelf beschermt tegen hackers.